Hunting a Ghost: On the Trail of an Elusive Adversary

EDUCAUSE Encore! • August 2018
Jodi Ito, UH Chief Information Security Officer
Melvin Quemado, UH Information Security Specialist
Agenda

• About the University of Hawaiʻi
• Timeline as the incident unfolded
• Incident Details
• Incident Remediation
• Organization Situational Awareness
University of Hawai‘i (UH) System

3 Four Year Campuses
- UH Hilo (Hawai‘i)
- UH Mānoa (O‘ahu)
- UH West O‘ahu (O‘ahu)

7 Two Year Campuses
- Hawai‘i Community College (Hawai‘i)
- Honolulu Community College (O‘ahu)
- Kapi‘olani Community College (O‘ahu)
- Kaua‘i Community College (Kaua‘i)
- Leeward Community College (O‘ahu)
- UH Maui College (Maui)
- Windward Community College (O‘ahu)

Students: 51,000+
Employees: 10,000+
Ever have one of those days?

We’ve had 341 of them since 9/15...

...and still counting!
Emergency Alert
BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.

Slide for more
URGENT. please call me on the cell at your earliest convenience.
Incident Response Timeline

• Friday, Sept. 15:
  • UH Researcher contacted by colleague
  • Researcher’s email account was compromised
  • Sent highly targeted spear phish contained malware-infected attachment
  • UH Researcher contacted CISO; blocked mail server ★
  • In parallel, CISO received “HEADS UP – condition RED!!” email from security colleague at the other institution
  • Spear phishing attachment was uploaded to VirusTotal ★
I think this is what you want?
Analysis of Malicious Attachment

• Malware embedded in the spear-phishing email’s attachment

• Payload exploited CVE-2017-8759; injecting SOAP WDSL parser code

• Downloaded and executed a script which contained a backdoor beacon; identified attacker’s IP

• .NET Framework Remote Code Execution Vulnerability, reported by FireEye on 09/12/2017
All Hand’s On Deck!

• UH Researcher deals with “defense-related” research
• Other recipients of spear phish also dealt with “defense-related” research
• Needed to identify root cause of compromised account quickly
Outlook Web Access Logs

- Attackers somehow acquired the UH Researcher’s email credentials

<table>
<thead>
<tr>
<th>Date</th>
<th>Attacker’s Action</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aug. 30</td>
<td>First login to UH Researcher’s email from external IP</td>
<td>~5 min.</td>
</tr>
<tr>
<td>Aug. 31</td>
<td>Failed login attempt to another UH email account from a UH IP</td>
<td>-</td>
</tr>
<tr>
<td>Aug. 31</td>
<td>Login to UH Researcher’s email account from a UH IP address</td>
<td>~48 min.</td>
</tr>
<tr>
<td>Sep. 01</td>
<td>Login to UH Researcher’s email account from a UH IP address</td>
<td>~1 hr. 20 min.</td>
</tr>
<tr>
<td>Sept 15</td>
<td>Login to UH Researcher’s email account from external IP address</td>
<td>~57 min.</td>
</tr>
</tbody>
</table>
Additional Information

• Eleven spear phishing emails were sent to 12 recipients (one was a Cc:) including other UH individuals
• Two UH individuals opened the malicious attachment but firewall rules were updated to block the attackers IP
• Seven UH IPs were found to be communicating with attackers IP
• Department conducts defense and maritime related research


Compromised Systems

- Seven (7) computers were observed communicating with the C&C

<table>
<thead>
<tr>
<th>IP</th>
<th>Role</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.171.XXX.XX</td>
<td>Staff PC</td>
<td>Windows 10</td>
</tr>
<tr>
<td>128.171.XXX.XX</td>
<td>Active directory / file server</td>
<td>Windows 2003</td>
</tr>
<tr>
<td>128.171.XXX.XX</td>
<td>Staff PC</td>
<td>Windows 10</td>
</tr>
<tr>
<td>128.171.XXX.XX</td>
<td>License server</td>
<td>Windows XP</td>
</tr>
<tr>
<td>128.171.XXX.XX</td>
<td>Staff PC</td>
<td>Windows 7</td>
</tr>
<tr>
<td>128.171.XXX.XXX</td>
<td>Staff PC</td>
<td>Windows 10</td>
</tr>
<tr>
<td>128.171.XXX.XX</td>
<td>Lab PC</td>
<td>Windows XP</td>
</tr>
</tbody>
</table>
And so it began...
Technical Details
Analysis of Windows XP SP3 PC
Analysis of Windows XP PC

• PC was exposed to the internet with remote desktop port (rdp) exposed

• Attackers immediately compromised machine and replaced sticky keys (sethc.exe) with command prompt (cmd.exe)
  • Renamed to sethc1.exe
Analysis of Windows XP PC

• Attacker downloaded and executed their backdoor
  • Remote Access Tool communicated to C&C
  • Created a copy cmd.exe into %TEMP% folder
    • Named this file, ‘system’

• Attacker staged and used multiple tools
Attacker Toolkit
Attacker Toolkit

- MT.exe
  - Capabilities include TCP port scanner
  - Ability to connect to other computers via SMB
- MimikatzLite
- NTDSDumpEx
- Pskill
- Pslist
- Dtunnel (Dog Tunnel) – SOCKS Proxy
- Responder
Modern OS Compromise

Windows 7 – Windows 10
Modern OS

- Attacker uses compromised credentials to log into computers
Persistence

- A service is created, usually tailored to the system
• The service executes a JavaScript file that downloads and runs Cobalt Strike using PowerShell
Periscope / Leviathan
APT Group
Attacker TTPs  
(Tactics, Techniques, Procedures)

- Two distinct backdoor methods:
  - Windows XP - StickyKey
  - Windows 7/10 - JS + Beacon (Beacon re-downloaded and executed each time the JavaScript is executed)

- Persistence methods include StickyKey, Task Scheduler, Windows Service

- Lateral movement methods appear to be focused around obtaining passwords via MimiKatz, SpiderLabs Responder, NTDSDumpEx, Shadow Copy > NTDS.dit > offline cracking

- Defense and evasion methods are hiding malware files in existing folders with legitimate-sounding names, running CMD via c:\windows\temp\system, deleting event logs, memory-only malware
Attacker TTPs

- Another (new?) method involves compromising the victim PC and executing a single JavaScript file.
- If this script executes, the only sign of infection is a running process called "wscript.exe" which is a legitimate Windows program.
- When the victim PC connects with the C&C, the main malicious script is downloaded into memory and executed.
- C&C commands are limited but enough to upload more powerful tools.
- Callback to the C&C is done via a cookie in GET request encoded in base64.
Attacker TTPs

• The Group also used a proxy called reGeorg (available from Github) to hide its origination during the first part of their campaign and later abandoned its use and accessed the PHP scripts directly.
More Reading

• F-Secure: NanHaiShu:
  • https://labsblog.f-secure.com/2016/08/04/nanhaishu-rating-the-south-china-sea/

• FireEye: TEMP.Periscope:
  • https://www.fireeye.com/blog/threat-research/2018/03/suspected-chinese-espionage-group-targeting-maritime-and-engineering-industries.html

✓• Proofpoint: Leviathan:
LEVIATHAN: ESPIONAGE ACTOR SPEARPHISHES MARITIME AND DEFENSE TARGETS

OCTOBER 16, 2017  Axel F, Pierre T

Overview
Proofpoint researchers are tracking an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe.
LEVIATHAN: ESPIONAGE ACTOR SPEARPHISHES MARITIME AND DEFENSE TARGETS

OCTOBER 16, 2017  Axel F, Pierre T

Key takeaways from this research include:

- **Industry targeting**: The actor targets defense contractors, universities (particularly those with military research ties), legal organizations [3] and government agencies [3]. The actor has particular interest in naval industries including shipbuilding and related research.

**Overview**

Proofpoint researchers are tracking an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe.
Delivery and Exploitation

*September 2017*

On September 15 and 19, 2017, Proofpoint detected and blocked spearphishing emails from this group targeting a US shipbuilding company and a US university research center with military ties. Example emails used the subject “Apply for internship position” and contained an attachment “resume.rtf”. Another attachment, “ARLUAS_FieldLog_2017-08-21.doc” contained a “Torpedo recovery experiment” lure. The attachments exploited CVE-2017-8759 which was discovered and documented only five days prior to the campaign [1].

Proofpoint researchers are tracking an espionage actor targeting organizations and high-value targets in defense and government. Active since at least 2014, this actor has long-standing interest in maritime industries, naval defense contractors, and associated research institutions in the United States and Western Europe.
Ongoing Incident...
• E-mails from foreign nationals with resumes and “web bugs” in them

Possible Reconnaissance

Dear [Name],

I am writing to express my interest in the postdoctoral position in [Field] at [Institution]. I am a recent graduate from [University] with a degree in [Major], and I am confident that my skills and experience make me a strong candidate for this role.

During my graduate studies, I was involved in several projects that required [specific skills or knowledge]. These experiences have prepared me well for the challenges of this position. In addition to my academic pursuits, I have also been involved in [related extracurricular activities or projects].

I am particularly interested in [specific aspect of the position]. In my [previous work or research], I [achieved or contributed to]. I believe that these experiences will be valuable in [potential contributions to the position].

I am confident that my background and skills align well with the requirements of this position. I am eager to contribute to [Institution] and believe that I can make a meaningful contribution in [specific areas or projects].

Thank you for considering my application. I look forward to the opportunity to discuss my qualifications further.

Sincerely,

Ming Zhang
Email: mingming@technoweb.com
Recommendations to UH Field

- Inventory computing assets
- Remove / Replace old systems/OS (XP, Server 2003)
- Check current systems for any of the discussed indicators
- Be suspicious of resumes (or unsolicited documents) from any source, don’t immediately share
- Close off remote login/access to the world capabilities (e.g. rdp, vnc, ssh etc.)
  - Simply moving the port doesn’t protect the system
- Use multi-factor authentication wherever possible; especially for privileged accounts
## Organizational Situational Awareness

### DATA GOVERNANCE & INFORMATION SECURITY

**UH Campus Briefings**

The UH community is invited to attend information briefings on data governance and information security. Topics covered are the growing information security threats to the University, updates on data governance and HIPAA policies.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
<th>Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friday, Feb. 9</td>
<td>1:30-3:30 p.m.</td>
<td>Hawai‘i CC - Manoa</td>
<td>Building 368, Room 101</td>
</tr>
<tr>
<td>Tuesday, Feb. 13</td>
<td>2:00-4:00 p.m.</td>
<td>Kapolei CC</td>
<td>O‘ahu Conference</td>
</tr>
<tr>
<td>Wednesday, Feb. 14</td>
<td>9:30-11:30 a.m.</td>
<td>Kaua‘i CC</td>
<td>Fine Arts Auditorium</td>
</tr>
<tr>
<td>Friday, Feb. 16</td>
<td>9:30-11:30 a.m.</td>
<td>UH Hilo</td>
<td>UCB 127</td>
</tr>
<tr>
<td>Wednesday, Feb. 28</td>
<td>9:30-11:30 a.m.</td>
<td>UH Mānoa</td>
<td>Campus Center Ballroom (seating available - details forthcoming)</td>
</tr>
<tr>
<td>Thursday, Mar. 1</td>
<td>9:00 -11:00 a.m.</td>
<td>Maui College</td>
<td>Kala‘ikea 105/105C</td>
</tr>
<tr>
<td>Tuesday, Mar. 6</td>
<td>9:30 -11:30 a.m.</td>
<td>Windward CC</td>
<td>Mānoa Room 101-103</td>
</tr>
<tr>
<td>Wednesday, Mar. 7</td>
<td>9:30-11:30 a.m.</td>
<td>UH West O‘ahu</td>
<td>Multi Purpose Room</td>
</tr>
<tr>
<td></td>
<td>1:00-3:00 p.m.</td>
<td>Leeward CC</td>
<td>ED Building, Room 201</td>
</tr>
</tbody>
</table>

---

### Additional Presentations:

- UH Community College Professional Development Institute Day
- Hawaii Student Success Institute
- Office of Research Services Certification
- UH Fiscal Administrators Quarterly Meeting
- UH Personnel Officers
- Annual All-Campus IT Workshop

Institutional Plans

- Incident Response Plan
- Incident SWAT team
- Communications Response Plan
  - Senior leadership
  - General Counsel
  - Public Relations
Beyond UH

• Ongoing investigation
• Not isolated to University of Hawaii
• Other institutions were affected
Questions?

Jodi Ito
UH Chief Information Security Officer
jodi@hawaii.edu

Melvin Quemado
UH Information Security Specialist
mquemado@hawaii.edu